A Study of Cyber Security, A Boon for Internet Security

Akanksha Yadav
Assistant Professor,
Department of Computer Science and Engineering,
University of Lucknow, Lucknow, Uttar Pradesh.

Abstract: Cyber Security is the protection of computer, data, networks, mobile devices from the malicious attack. To secure the information from the hackers is the biggest challenge for the world. Whenever we listen the word ‘cyber security’ the initial thing which strike in our mind is ‘cyber crimes’. As the world is going digital the incidence of cyber-crime is increasing. To prevent the cyber-crimes, Various Governments and companies are planning to stop it. Cyber security is a matter of concern for many companies, despite many measures.

Index Terms: cyber security, cyber-crime, social media, cloud computing, android apps.

I. INTRODUCTION
People can send any data e.g. audio, video, images etc. Through a just single click, did you ever think the transmitted data is secure or not? Due to much use of technologies we are not too able to save our confidential information. Mostly business transaction are doing online transaction, for the online transaction it require more security. Sometimes, transaction are not secure. For transaction cyber security became the ultimate issue. All the technologies like net banking, mobile computing etc. they need high level security. These technology stores the all the information of a person like their name, contact no., Account number, Pan number etc., high level security is most imp for them. To protect the confidential information of any person is the essential thing for any nation. Along with the development of applications, securing the internet has also become a part of the government policy. Government should also give the right to the enforcement agencies to investigate about the cybercrime.

II. CYBER CRIME
Cybercrime is a type of crime in which computer is a object, crime (phishing, hacking etc.), it is used according to as a tool for any offense or crime like identity theft, steal the information, online fraud etc. The crime which is done through the internet is called cybercrime. Cyber criminals used computers and internet to steal the information of person or access the business trade. There are many privacy concerns surrounding cybercrime when confidential information are grab or disclosed.

III. CYBER SECURITY
To keep the data secure and confidential is always the first priority of the any organization. We are living in a world where all the data are stored digitally. While using the social networking sites users feel free to interact with their friend, they share images and videos also, they also share the things which is happening in their life but it’s not safe. Hackers can easily steal anyone’s information through the social media. Transaction is also not secure that’s why it need more security.

Ways to Prevent Cyber Attacks:
• Install, use and regularly update the antivirus on every computer which is used in offices or home.
• Use a firewall for the internet connection.
• Make backup copies of important data.
• Secure wifi networks.
• Regularly change password.

IV. TRENDS CHANGING CYBER SECURITY
There are some technologies that are having impact on cyber security;

1) Web Server: All the websites are hosted on the web server. It stores the database of the website. The main work of the web server is to store, process and deliver web pages to the client. The ultimatum of attack on the web application to extract data attackers can attack through the malicious code. Web server are the best platform for the criminals to steal the information of the any person. We should always use a secure browser for the transactions.

2) Cloud Computing: If someone provide the service through the internet is called cloud computing. It can be any service like offsite storage or computing resources. Now a day’s mostly companies are adopting cloud services. More use of cloud computing is a big issue for cyber security. Number of applications are increasing in cloud grows, policy etc cloud services also need to secure the loss of information. Cloud services are creating their own model but still the security issues are being raised.

3) Mobile Network: Every person is using mobile phones they can communicate to each other in the entire world. Mobile network is a wireless communication. The use of firewall and other security measures are decreasing because the number of mobile, tablet users are increasing. It require more security. we must think about the security issue of mobile network. Never try to connect unauthorized Wi-Fi.
IPV6: (Internet protocol version 6): IPV6 was developed by Internet Engineering Task Force to replace the IPV4. IPV6 is the most recent version of Internet Protocol. IPV6 is a L3 (third layer) protocol that allows communication and data transfer to take place over the internet. It is more secure as compare to IPV4.

Cyber Security Techniques:

- **Access Control**: Access control is a type of electronic Security Technology. Through access control, we can control a person who is coming to a particular place and keep the data of all the persons.

- **Authentication**: It is the process of identity of a user by obtaining some sort of credential and using those credentials to verify the user’s identity, if the credentials are valid the authorization process start.

- **Malware Scanner**: It is a software which is used to scan the files and the documents which are store in the system from the viruses, virus, worms and Trojan horse are the example of malicious software

- **Antivirus Software**: Antivirus software is also known as Anti Malware, Anti-virus software is a program which are designed to prevent, detect or remove software issues from the system.

V. CONCLUSION

- As the technology continue to grow incident of cyber-crime is also increasing day by day. We will have to protect ourselves from the frauds never click on the suspicious link if we click on this link the hackers access all your information.

- Update anti-virus in the system and also update yourself to prevent this type of crime.

REFERENCES


[10] Isabella Biscoglio, Giuseppe Lami, Eda Marchetti and Gianluca Trentanni Institute of Information Science and Technologies “Alessandro Faedo” of the National Research Council, Pisa, Italy.


